Berkeley Barb

FOR MACHINE SALE ONLY

Issue 484, November 22-28, 1974 | PUBLISHED EVERY FRIDAY | 204 | Copyright Berkeley Barb 1974 | Bay Area 25c Elsewhere 50c

SF Bay Media All Shook Up

ANTI-RAPE

No More Arrests For Berkeley Pot?

Drawing by Jane Norling, from 'Women of Viet Nam', Peoples Press

THE IBM PAPERS

PART 2:

The material on these pages concludes the IBM Papers, which were obtained for the Berkeley Barb by the New York News Service. The first part of the document, printed in last week's Barb, dwelt on "the spectrum of real terrorist threats against IBM," with particular reference to their installations in the United States. Then the document focussed on counter-measures, emphasizing the development of "an effective intelligence system on the plans and acts of extremists and terrorists." Urging that the "inherent weaknesses of terrorists and extremists" be maximized, the paper listed Carlos Marighella's The Seven Sins of the Urban Guerrilla. Now read on.

IBM

POLICE

INTERNATIONAL BUSINESS MACHINES
AND
INTERNATIONAL ASSOCIATION
OF CHIEFS OF POLICE

Security: A Management Style
A Course of Instruction in Corporate Protective Services

IBM AS A TARGET FOR TERRORISTS

CONSTRAINTS & CONSIDERATIONS

-10-

The apparent absence of dramatic acts should not divert attention from the need to be sensitive to any acts of extremists and terrorists. Does IBM currently possess an intelligence system adequate to detect, report, and analyze even seemingly minor incidents, at all of its far-flung Sites? An adequate early warning system will be able to monitor even trivial events, and to examine these events—which may be occurring at Sites far apart—for trends, and for indications of more substantial pressures.

The vocabulary of terrorism is not fully precise, as indicated in the simultaneous use of "extremist" and "terrorist", to describe a range of behavior. The term "terrorist" has somewhat more propaganda wallop than the term "extremist", although U.S. Government agencies find today that they are under some pressure to avoid using the term "extremist".

IBM may be particularly vulnerable to attempts to set a *scapegoating cycle* in process. As the level of terror rises, any large, "strong" organization will find itself under pressures to cease doing the "unreasonable" things that lead to terrorism, and to make "reasonable" concessions to

cal power in a number of states, and its National Chairman in May, 1974, described the NCLC as the third major political force in the world. (He perceives the other two to be the "Rockefeller-CIA complex" and the Soviet Politburo. Note the characteristic extremist self-aggrandizement through choice of "big" enemies.)

Note that the NCLC rhetoric in this editorial tries to achieve a certain chatty, "worker's" style (as an intensely intelligent Leftist might imagine workers to talk). There is little in it about the potential role of violence in advancing the working class movement. Those who encounter NCLC and similar operatives are likely to feel initially somewhat baffled, in that the encounter is likely to center at first on words. Only later may it become clear that the organizers are contriving physical encounter situations, in which Corporate personnel may be trapped and Corporate facilities exposed. The truly skilled *provocateur* of violence will try to establish a legitimate, peacefully verbal demonstration, as his take-off point for a cycle of escalating verbal and physical abuse.

CONSTRAINTS & CONSIDERATIONS

-12-

The JDL's activities present a special challenge to IBM, many of whose more creative individuals will identify strongly with Israel's aspirations. The Corporation needs to consider its stance on the Arab-Jewish question in this light and with particular care. A pro-Israeli stance will be internally satisfying and will minimize JDL threats. Will it, however, make the Corporation increasingly vulnerable to Arab strike tactics?

commune is a face-to-face group of intensely involved individuals, working in and among similar groups, conventional law enforcement techniques of surveillance and penetration are severely limited. Thus, intelligence about them is likely to be incomplete and sometimes misleading.

In view of this, how is a Corporate intelligence system going to be given timely advice about possible threats from these groups?

By and large, even the more paranoid American restorationists do not have many reasons to be upset with IBM—but this does not mean things won't change. Restorationist populists could, in the future, find IBM's scope and its technology to be threatening. More likely restorationist incursions are to be expected from *particularistic* groups, who have a specific grievance.

Here, whether it is facing the JDL, the American Nazis, the Klan, or others, Site security specialists should try to establish direct dialogue with restorationist agitators and work to give them a safe haven off Corporate property, where they can defuse their anger and anxieties.

This is another reason for training Site security people in encounter techniques, and for making sure that those schooled in encounter techniques also know how to work in tandem with law enforcement agencies on additional responses and countermeasures.

Terror is no justification for terror, although an answer to terror tactics may require skillful coordination of a range of physical countermeasures.

The options to be discussed here are general. They are stated here in the form of guidelines for specific later implementation at CHQ and Site

CONSTRAINTS & CONSIDERATIONS

-14-

The range of possible terrorist and extremist actions is potentially broad. This dictates an intelligence system adequate for monitoring the entire threat spectrum. But, there will be substantial resistance to anything that smacks of "intelligence gathering"—and even more to anything covert or "spooky". IBM at CHQ and Site levels thus will face some hard decisions about how to define and institutionalize this very necessary intelligence capability.

An important element of a counter-terror intelligence system will be its ability to generate analyses of incident data. Deriving from these analyses should be projected response scenarios. IBM is unusually well qualified to develop such scenarios. In doing so, it can draw upon accumulated expertise within the Defense research and development community.

One generalized position within IBM's projected security career path might well be the role(s) of "security response analyst/security response

things that lead to terrorism, and to make "reasonable" concessions to terrorists. Particularly difficult to manage will be "Robin Hood" terrorists, who have access to the media—one of many reasons for IBM's thinking now about how to deny terrorists use of the media to communicate propaganda against the Corporation. This thinking may run against the grain of those IBMers who believe in a completely free Corporate information policy.

One of the essential elements of a counter-terror campaign is to define an acceptable public image, in the face of terrorist efforts to reshape the organization's prior image. This campaign will necessarily have a strong propaganda element in its own right, a fact which must be accepted and understood.

Generally viewed, radical extremists are likely to want more from IBM than restorationists—but both major groups are likely to want something in the future. The difference between radicalism and restorationism as extremist movements centers critically on the content of *ideologies*. The ideology of a group remains a critical indicator of what it will do, in spite of one main line of extremist group analysis, which tends to hold that right-wing extremists can be viewed as "radical", partly because they join radicals in using extreme methods. Indeed, both in methods and in certain latent themes of populism, right-wing and left-wing extremists do exhibit similarities. The net result of looking at the Right as Radical is, however, to obscure continuing and significant differences in ideology between the Right and Left in American society.

CONSTRAINTS & CONSIDERATIONS

-11-

Too much can be made of the urban guerrilla's imaginings that a society is vulnerable through its few concentrations of economic and political power. As Marighella himself notes and as others (including Chairman Mao) have written, the long term revolution in an underdeveloped society is impossible without mobilizing the rural masses.

The special lesson of urban guerrilla thinking remains, however, that skilled terrorists, equipped with a revolutionary plan, can strike effectively at those complex business enterprises that necessarily focus their activities in the urban core of *any* society.

The United States is somewhat more difficult to judge as a potential setting for terrorist violence against IBM. The prospects of armed terrorism appear fewer than overseas, yet within the radical extremist underground, there are known to be many individuals who have the technical and ideological disposition to strike at organizations such as IBM.

Sound intelligence doctrine holds that IBM should now be monitoring various sources, for indications of this kind of activity. Can—and ought—IBM bring itself to do so?

The NCLC is precisely the kind of organization which IBM should be closely monitoring, using all its resources.

IACP analysts have also naturally been interested in the NCLC. They have found that NCLC began as the "Students for a Democratic Society Labor Committee". Today, it is trying to pick up the various pieces of the Left. It is active in more than 40 U.S. cities and has overseas branches in Italy, Sweden, France, West Germany, and Canada. At one time, NCLC used physical attacks on members of other communist and socialist groups during meetings and conventions, in an effort to weaken these rivals. These efforts were largely unsuccessful, but the results have done little to diminish NCLC's view that violence is a necessary component in the process of establishing socialism. The NCLC is moving to gain politi-

Simply because it operates overseas, IBM will have some vulnerability to terrorist violence there. Add to this simple fact of location the fact that IBM is identified with Western technological supremacy and, to some degree, with so-called "American Imperialism", and the overall assessment of IBM's future overseas vulnerability must be placed relatively high on a scale of judgments.

South America is probably the most important single source of the theory now influencing terrorist violence around the world. Marighella's *Minimanual* is a minor classic, widely read in the Western Hemisphere. As one bibliographic source for this Block emphasizes, however, there is a possibly critical conceptual difference between the urban guerrilla and the terrorist:

> . . . Urban guerrilla warfare can be defined as criminal conduct for revolutionary purposes. Terrorism, on the other hand, is violent criminal activity designed to intimidate for political purposes. The distinction is in goals sought and sometimes in methods used. The guerrilla is working toward revolution. The terrorist acts to focus attention on a particular grievance.
>
> (U.S. Federal Bureau of Investigation, "Trends in Urban Guerrilla Tactics", *FBI Law Enforcement Bulletin*, July, 1973, p. 2.)

In practice, the line between terrorism and the urban guerrilla is not as neat. In fact, many little terrorist groups love to preen themselves with the thought that they are "urban guerrillas"; part of their nourishment comes from this fantasy. Indeed, the whole thrust of Symbionese rhetoric was *they were urban guerrillas*, and for a time during the late Winter and early Spring of 1974, American institutions were responding as if they were. On the other hand, urban guerrillas fully recognize the value of indiscriminate terror tactics.

The kidnapping of Victor Samuelson has become a classic in the use of a hostage to achieve political ends.

Assume that IBM, on strictly humanitarian grounds, insists that it must always keep open the possibility of ransoming any of its kidnapped personnel. Consider now the profoundly destabilizing effects of over $14 million in the hands of the ERP—if, indeed, they used part of the money to fund a "Revolutionary Coordination Board". Under these conditions, what is the tradeoff between the need to save an executive and the need to arrest a long term assault on the whole structure of the capitalist system? A tough question, at best.

CONSTRAINTS & CONSIDERATIONS

-13-

All IBM security specialists facing NCLC probes should be thoroughly versed in controlling encounter situations at varying levels of intensity.

The "tight collective" is an important organizational innovation, for those radical extremists who are anarchistic, and who at the same time wish to have the tactical advantages conferred by disciplined teamwork. The Symbionese were clearly such a tight collective. Merely to call oneselves an "Army" does not impose hierarchical discipline on a group. (See Vestermark, 1974, p. 20, which is Figure 1.)

Tight collectives exist principally in major urban centers where there is a large communal "dropout" population. Here, fugitives and terrorists can with some ease be "passed along" within a relatively loosely structured horizontal network of tight collectives. Since each collective or

might well be the role(s) of "security response analyst/security response manager". Needless to say, there is an interesting—and sticky—question about whether and when and how these people might assume *operational* roles. The question is not confined to IBM.

Even with effective intelligence and analysis, an organization's response may be slow and uncoordinated, thus conferring crucial advantages on terrorists. A centralized action directorate, close to top management and with the ability to reach quickly to Site, would offer critical managerial capabilities in mounting timely, flexible responses.

As with the intelligence system: How would the capabilities implied by an "action directorate" be institutionalized within IBM? What internal fears will it create? How can it be kept from degenerating into a vehicle of internal Corporate discipline? (Note here the tragic history of the Ford Motor Company, during the last years of its Founder.)

The third guideline implies that IBM will develop a number of specific options, based on a number of policy decisions. In some cases (bomb threats, for example), Sites have been developing response procedures. In other cases (most notably, perhaps, kidnap/hostage actions), fundamental issues appear to remain unresolved. Note that there must be a close wedding of policies and procedures in developing these response options. A small analytic group, close to the "action directorate" and top management, might have the task of actually developing these options.

What would be the scope and limits of such a group?

Considering a response to kidnapping raises most of the important questions in developing counter-terror tactics and scenarios. The basic question here is: How far does IBM really want to go in building a carefully defined, combined capability for responding to acts of terrorism and extremism? If it wishes to stay short of developing full response capabilities, then how can individual resources and policies be defined now, and held in readiness? Remember—that there is no real "book" on terrorism, and that it is very hard to keep capabilities "on the shelf" for

CONSTRAINTS & CONSIDERATIONS

-15-

later use. The essence of an effective response to terrorism is in speedy, coordinated, relevant action, by a response system maintained in a readiness posture.

Terrorists and extremists like to cultivate a folklore image of invincibility, as the prattle of the Symbionese clearly demonstrated. Marighella himself was sensitive to the problems this fantasizing creates for terrorists, and his "Seven Sins" are directed largely to overcoming this problem.

The Seven Sins reveal the tremendous psychological pressures under which terrorists and "urban guerrillas" operate. Security specialists should realize that not only do the Seven Sins suggest general psychological and strategic vulnerabilities which they might exploit, but that they offer clues about ways in which to force the tactical hands of terrorists.

This can lead to projecting potential covert counter-terror operations. Under what circumstances would IBM be justified in covertly exploiting Marighella's Seven Sins? If there were certain circumstances, how would they be defined, and what would be the nature of the covert operation(s)?

Sins 3 through 7 offer many possibilities for potentially effective—and potentially disastrous—covert operations. Certainly in the domestic setting, IBM security people will want to view these Sins, as well as Sins

continued on page 12

1 and 2, as potential weaknesses which can place valuable intelligence information in their hands. Within the United States, this may be just about the limit of the implications to be drawn from the Seven Sins. Note the dangers inherent, for example, in the comment on Sin 6.

In any case, Marighella's Seven Sins do not imply a full-blown counter-terror strategy. In the light of the dangers of covert operations, they may, in fact, be invitations to disaster. But--they do suggest many exploitable psychological pressures which exist within terrorist and extremist groups. These pressures should be considered in developing counter-terror strategies and tactics.

CASE HISTORY

-16-

THE PROBLEM

You manage security at Site R, where general products, systems development, and special Federal systems activities are conducted. About 4,000 employees are on the Site. You do not now have a systematic program for dealing with terrorist or extremist activity, because you understand that the Corporation wants a low profile security program.

During the last two months, a number of unusual events have occurred at your Site. One was a bomb threat, in which a female "Weatherperson" stated that the "Weather Underground" had planted a bomb inside your Administration Building. In fact, one went off – outside, spraying fragments into several people who had been evacuated from the Admin Building in response to the threat. The device had been artfully hidden in an ornamental shrub close by one of the side walls.

Then, you have had persistent reports of work slowdowns and sabotage from production managers. It is not possible to verify all of these, but in several employee recreation areas near Buildings where slowdowns have been reported, you discover a number of Klan documents, all advancing the theme that the Corporation is "Jew-controlled" and that all "honest God-fearing White People" should be "careful about making too much money for the Jews". In one assembly area, you have found evidence that a number of critical systems have been incorrectly wired and installed. In another area, the power cables to a drying oven have been cut.

Most recently, you have seen indications of agitation and provocation just outside the Site boundaries. There, some sort of "workers' organization" is calling for a greater voice in Site management. The organizers have handed out clever little IBM cards, with the inscription: "Are you just another hole to be punched?" These have gotten all over the plant and also into a neighboring high school. You know they are in the high school because sons and daughters of middle management at the Site are bringing them home to their parents, and complaining about the teasing and taunts they are getting at school.

All of this has come to the attention of local and regional news media, whose representatives have been asking you and Site Management for a "story" on the "problems" at the Site. You are wondering what to do, about both this request and other worries, and as you are wondering, a secretary comes running breathlessly to tell you that someone has "taken a shot" at one of the senior Site production managers.

ALTERNATIVES

-17-

The alternatives presented here have been phrased as general guidelines, rather than as precise action alternatives, although each major guideline directly implies immediate, specific measures. The alternatives can be viewed individually or, taken together, as constituting the beginning of a program for controlling terrorism and extremism.

Four alternatives in the form of guidelines were presented here:

1. *Develop an effective intelligence system* on the plans and acts of extremists and terrorists;

NOTES

2. *Centralize and coordinate the response* to terrorism and extremism, without destroying necessary tactical flexibility at the local level;

3. *Have multiple, flexible response options* for a variety of contingencies;

4. *Maximize the inherent weaknesses* of terrorists and extremists.

As in other Blocks of this course, development of any one of these alternatives implies major Corporate policy decisions. Taken together, these four guidelines point toward a potentially formidable intelligence and countermeasures apparatus. The willingness of security specialists and Corporate leadership to develop this kind of organizational counter-terror weapon may depend on events which lie only in the future. As events unfold, however, the basic lesson of the hypothetical Case History may become clearer: that only a carefully orchestrated, tightly controlled and disciplined total program can effectively cope with manifestations of extremism and terrorism.

RELATING THE PRINCIPLES

-18-

Terror does not justify terror, and IBM will be wise to retain its commitments to individual privacy and integrity as it considers possible countermeasures to terrorist activities. The more serious acts of terrorism against IBMers are likely to occur overseas, where fully developed "urban guerrilla" actions may occur. These will require a quasi-military response, and a tightly organized response capability. Domestically, the threats of terrorists and extremists may be less grave, but somewhat broader in their potential range.

At the very least, the Corporation must have certain contingency responses in readiness, to meet terrorist and extremist probes. An effective intelligence system is a must, and every security specialist should be able to make timely requests for data and analyses from it. Beyond this, every security specialist should be schooled in techniques used by terrorists and extremists to generate encounter situations. Every Site should be able to mobilize an "action directorate", which can deploy and manage responses to:

– persistent bomb threats;

– possible sabotage of its technology;

– kidnap/hostage and coercive bargaining situations;

– blackmail attempts at extortion;

– group assaults on its Sites;

– agitation intended to disrupt work and to set management against other personnel.

Counter-terror intelligence and potential action responses should be monitored closely at CHQ level. There, a centralized "action directorate" may be needed, to process intelligence, generate response options, and insure that all counter-terror activities, projected as well as ongoing, closely adhere to basic Corporate policies – particularly as policies begin to evolve or shift in response to events. Liaison between Corporate and Site "action directorates" must be quick and constant, with appropriate "fail-safe" provisions to insure that counter-terror actions will not degenerate into lawless or terroristic acts in their own right.

Many of the general problems created by the need to respond to terrorists come to a sharp focus in the issue of Executive Protection, the next Block in this Course. Indeed, the problem of developing an appropriate executive protective program can be viewed as a special case in the issues which have been raised in this Block. Just as an organization moving against terrorists must not become terrorists, so must those who need to protect a key organizational figure not end up by stifling that felt sense of freedom which is essential to his creativity.